

Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Никишкина Татьяна Юрьевна
Должность: Директор
Дата подписания: 30.01.2022 14:36:21
Уникальный программный ключ:
0a44cc3e5f5bb746f50173cba89518ff43040635

ФЕДЕРАЛЬНОЕ АГЕНТСТВО МОРСКОГО И РЕЧНОГО ТРАНСПОРТА

**ОМСКИЙ ИНСТИТУТ ВОДНОГО ТРАНСПОРТА (ФИЛИАЛ)
ФЕДЕРАЛЬНОГО ГОСУДАРСТВЕННОГО БЮДЖЕТНОГО
ОБРАЗОВАТЕЛЬНОГО УЧРЕЖДЕНИЯ ВЫСШЕГО ОБРАЗОВАНИЯ
«СИБИРСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ВОДНОГО ТРАНСПОРТА»**

УТВЕРЖДАЮ

Заместитель директора по УиНР ВО
ОИВТ (филиал) ФГБОУ ВО «СГУВТ»

_____ Калекин В.В.

« ____ » _____ 20 ____ г.

Шифр дисциплины: _____ . _____
(шифр ОПОП) (шифр дисциплины из учебного плана)

Рабочая программа дисциплины (модуля)

Наименование дисциплины (модуля):

Основы криптографии

(полное наименование дисциплины (модуля), в строгом соответствии с учебным планом)

Омск

_____ 2022
(год набора)

Составлена _____ доцентом _____ кафедры _____ ЕНиИТ
(должность) (сокращенное наименование кафедры)

_____ , _____ О.Л. Курнявко
(ученая степень) (ученое звание) (И.О. Фамилия)

_____ О.Л. Курнявко « _____ » 20 _____ г.
(подпись) (И.О. Фамилия) число месяц год

Рассмотрена и одобрена на заседании кафедры естественных наук и
информационных технологий

(наименование кафедры полностью)

от « _____ » 20 _____ г., _____
число месяц год

Зав. кафедрой _____ ЕНиИТ _____ О.Л. Курнявко
(сокращенное наименование кафедры) (подпись) (И.О. Фамилия)

Согласована:

Руководитель ОПОП _____ К.Т.Н. _____ Т.Л. Иванова
(ученая степень, ученое звание) (подпись) (И.О. Фамилия)

Заведующий библиотекой ОИВТ _____ И.Д. Скоробогатова
(подпись) (И.О. Фамилия)

1 Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с планируемыми результатами освоения образовательной программы

1.1 Цели дисциплины

Целью данной дисциплины является формирование у студентов фундамента естественно-научных знаний, базирующихся на законах природы, правильных представлений о современной картине мира, а также навыков применения физических законов к прикладным задачам современной техники.

1.2 Перечень формируемых компетенций

В результате освоения дисциплины (модуля) у обучающегося должны сформироваться следующие компетенции, выраженные через результат обучения по дисциплине (модуля), как часть результата освоения образовательной программы (далее – ОП):

Компетенция		Индикаторы освоения компетенции
Шифр	Содержание	
УК-1	Способен осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач.	УК-1.1. Знать: методики поиска, сбора и обработки информации; актуальные российские и зарубежные источники информации в сфере профессиональной деятельности; метод системного анализа. УК-1.2. Уметь: применять методики поиска, сбора и обработки информации; осуществлять критический анализ и синтез информации, полученной из разных источников; применять системный подход для решения поставленных задач. УК-1.3. Владеть: методами поиска, сбора и обработки, критического анализа и синтеза информации; методикой системного подхода для решения поставленных задач.
ПК-3	Способность оценивать качество программного обеспечения, в том числе проведение тестирования и исследование результатов.	ПК-3.1. Знать современные технологии, подходы, стандарты оценки качества разрабатываемого программного обеспечения. ПК-3.2. Знать базовые техники проектирования и комбинаторики тестов; классификации видов и типов тестирования, инструменты выполнения тестов. ПК-3.3. Уметь понимать процесс тестирования программного обеспечения; анализировать тестовые случаи, сопоставлять и анализировать информацию, проводить сравнительный анализ. ПК-3.4. Иметь навыки изучения плана тестирования и выявления приоритетных областей покрытия тестовыми случаями; выполнения необходимых видов тестирования в соответствии с планом тестирования; анализа полученных результатов.

2 Место дисциплины (модуля) в структуре образовательной программы

Дисциплина (модуль) реализуется в рамках вариативной части
(базовой, вариативной или факультативной)

основной профессиональной образовательной программы.

3 Объем дисциплины (модуля) в зачетных единицах (ЗЕ) с указанием количества академических или астрономических часов, выделенных на контактную работу обучающихся с преподавателем (по видам учебных занятий) и на самостоятельную работу обучающихся

Для очной формы обучения:
(очной, очно-заочной или заочной)

Форма контроля					з.е.		-	Итого акад. часов					Курс 4 Сем. 7									
Экзамен	Зачет	Зачет с оц.	КР	Контр.	Экспертное	Факт	Часов в з.е.	Экспертное	По плану	Контакт часы	СР	Контроль	з.е.	Итого	Лек	Лаб	Пр	КСР	КоР	КРП	СР	Контроль
6				66	6	6	36	216	216	94	86	36	6	216	32	32		10	20		86	36

Для заочной формы обучения:
(очной, очно-заочной или заочной)

Форма контроля					з.е.		-	Итого акад. часов					Курс 1										Курс 2									
Экзамен	Зачет	Зачет с оц.	КР	Контр.	Экспертное	Факт	Часов в з.е.	Экспертное	По плану	Контакт часы	СР	Контроль	з.е.	Итого	Лек	Лаб	Пр	КСР	КоР	КРП	СР	Контроль	з.е.	Итого	Лек	Лаб	Пр	КСР	КоР	КРП	СР	Контроль

4 Содержание дисциплины (модуля), структурированное по темам (разделам) с указанием отведенного на них количества академических часов и видов учебных занятий

4.1 Разделы и темы дисциплины (модуля) и трудоемкость по видам учебных занятий (в академических часах)

№	Разделы и темы дисциплины (модуля)	Виды учебных занятий, включая СРС											
		Лек			Лаб			Пр			СРС		
		О	ОЗ	З	О	ОЗ	З	О	ОЗ	З	О	ОЗ	З
1.	Кодирование информации	6			6						18		
2.	Симметричное шифрование	6			6						18		
3.	Асимметричное шифрование	6			6						16		
4.	Электронная подпись	6			6						18		
5.	Защита данных в информационных системах	8			8						16		
ИТОГО		32			32						86		

Примечания: О – очная форма обучения, ОЗ – очно-заочная форма обучения, З – заочная форма обучения.

4.2 Содержание разделов и тем дисциплины

1. Кодирование информации

Основные понятия: задачи, объект, предмет, методы криптографической безопасности. Политика в сфере обеспечения информационной безопасности России. Концептуальная модель информационной безопасности. Составляющие концептуальной модели информационной безопасности. Современная концепция информационной безопасности. Цели защиты информации. Носители защищаемой информации. Понятие информации.

2. Симметричное шифрование

Простейшие методы шифрования с закрытым ключом. Общая схема симметричного шифрования. Методы замены. Пропорциональные шифры. Многоалфавитные подстановки. Методы гаммирования. Методы перестановки. Понятие композиционного шифра. Операции, используемые в блочных алгоритмах симметричного шифрования. Структура блочного алгоритма симметричного шифрования. Методы симметричного шифрования. Блочное и потоковое шифрование.

3. Асимметричное шифрование

Основные понятия и классификация средств асимметричной криптографии. Основные свойства асимметричных криптосистем. Предпосылки создания методов шифрования с открытым ключом и основные определения. Односторонние функции. Требования к алгоритмам шифрования с открытым ключом. Использование асимметричных алгоритмов для шифрования. Цифровая подпись на основе алгоритмов с открытым ключом. Генерация и хранение ключей. Формирование секретных ключей с использованием асимметричных алгоритмов. Распределение ключей. Управление ключами в системах с открытым ключом. Алгоритм Диффи-Хелмана. Алгоритм RSA. Алгоритм Эль-Гамала. Криптографические системы на эллиптических кривых. Возможные атаки при использовании алгоритмов асимметричного шифрования.

4. Электронная подпись

История развития. Виды электронных подписей в Российской Федерации. Общая схема электронной цифровой подписи. Использование хеш-функций. Виды асимметричных алгоритмов цифровой подписи. Электронная подпись на основе алгоритма RSA. Цифровая подпись на основе алгоритма Эль-Гамала. Стандарты на алгоритмы цифровой подписи. Стандарт цифровой подписи ГОСТ Р34.10-94. Новый отечественный стандарт ЭЦП. Управление открытыми ключами.

5. Защита данных в информационных системах

Основные подходы к измерению информации. Энтропия и неопределенность. Норма языка и избыточность сообщений. Понятие совершенно секретной системы. Расстояние единственности.

4.3 Содержание лабораторных работ

Раздел (тема) дисциплины	Тема лабораторной работы
Кодирование информации	Лаб. №1
Симметричное шифрование	Лаб. №2
Асимметричное шифрование	Лаб. №3
Электронная подпись	Лаб. №4
Защита данных в информационных системах	Лаб. №5

4.4 Содержание практических занятий

Дисциплина не предусматривает практические работы.

4.5 Курсовая работа

Дисциплина не предусматривает курсовую работу.

4.6 Курсовой проект

Дисциплина не предусматривает курсовой проект.

4.7 Самостоятельная работа. Контроль самостоятельной работы

В самостоятельную работу студента входит подготовка к занятиям по дисциплине путём изучения теоретического материала по источникам, указанным в перечне основной и дополнительной литературы, выполнение практических работ, оформление практических заданий и подготовка к их защите.

Контроль самостоятельной работы осуществляется в ходе практических и лабораторных занятий.

4.8 Интерактивные формы обучения

В процессе освоения данной учебной дисциплины интерактивные формы используются при изучении следующих тем:

Раздел (тема) дисциплины	Количество часов		
	О	ОЗ	З
Кодирование информации	2		
Симметричное шифрование	-		
Асимметричное шифрование	-		
Электронная подпись	2		
Защита данных в информационных системах	2		
Итого	6		

5 Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине (модулю)

5.1 Описание показателей и критериев оценивания компетенций, описание шкал оценивания

Показатели оценивания	Описание показателя
Оценка «отлично» (зачтено)	Обучаемый демонстрирует способность к полной самостоятельности (допускаются консультации с преподавателем по сопутствующим вопросам) в выборе способа решения неизвестных или нестандартных заданий с использованием знаний, умений и навыков, полученных в ходе проведения освоения дисциплины, следует считать компетенцию сформированной на высоком уровне. Присутствие сформированной компетенции на высоком уровне означает способность студента к ее дальнейшему саморазвитию и высокой адаптивности практического применения к изменяющимся условиям профессиональной задачи.

Показатели оценивания	Описание показателя
Оценка «хорошо» (зачтено)	Обучаемый демонстрирует самостоятельное применение знаний, умений и навыков при решении заданий, аналогичных тем, которые предоставлял преподаватель при потенциальном формировании компетенции, подтверждает наличие сформированной компетенции, причем на более высоком уровне. Наличие сформированной компетенции на повышенном уровне самостоятельности со стороны обучаемого при ее практической демонстрации в ходе решения аналогичных заданий следует оценивать как положительное и устойчиво закрепленное в практическом навыке.
Оценка «удовлетворительно» (зачтено)	Обучаемый демонстрирует самостоятельность в применении знаний, умений и навыков к решению учебных заданий в полном соответствии с образцом, данным преподавателем, по заданиям, решение которых было показано преподавателем, следует считать, что компетенция сформирована, но ее уровень недостаточно высок. Поскольку выявлено наличие сформированной компетенции, ее следует оценивать положительно, но на низком уровне.
Оценка «неудовлетворительно» (не зачтено)	Обучаемый не способен самостоятельно продемонстрировать наличие знаний при решении заданий, которые были представлены преподавателем вместе с образцом их решения, отсутствие самостоятельности в применении умения к использованию методов проведения пред- дипломной практики и неспособность самостоятельно проявить навык повторения решения поставленной задачи по стандартному образцу свидетельствуют об отсутствии сформированной компетенции.

5.2 Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений и (или) навыков, характеризующих этапы формирования компетенций в процессе освоения образовательной программы

Качественный вопрос: привести ключевые требования кодирования информации.

Задача: оценить трудоемкость взлома 256-битного ключа.

Задача: предложить модель шифрования сеанса коммуникации.

5.3 Перечень вопросов для итогового контроля по дисциплине

1. Кодирование информации
2. Симметричное шифрование
3. Асимметричное шифрование
4. Электронная подпись
5. Защита данных в информационных системах

5.4 Методические рекомендации к проведению итогового контроля по дисциплине

На итоговый контроль выносится учебный материал, рассмотренный на лекционных и практических занятиях, а также темы, которые были предложены для самостоятельного изучения.

Формой проведения итогового контроля по данной дисциплине является экзамен и дифференцированный зачет, которые проводятся в устной форме с использованием билетов, содержащих теоретическую и практическую часть. Также допустимо проведение итогового

контроля в письменной форме. О форме проведения итогового контроля студенты должны быть оповещены заблаговременно.

Во время подготовки к ответу на экзамене использование справочной литературы не допускается.

6 Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины (модуля)

6.1 Основная учебная литература

1. Башлы П. Н. Информационная безопасность и защита информации [Электронный ресурс]. - Москва: Евразийский открытый институт, 2012.
2. Партыка Т. Л. Информационная безопасность. - М. : Форум, 2011.
3. Чмора, А.Л. Современная прикладная криптография. - М.: Гелиос АРВ, 2001.

6.2 Дополнительная учебная литература

1. Ищейнов В.Я. Организационное и техническое обеспечение информационной безопасности. Защита конфиденциальной информации. - М.: Форум : ИНФРА-М, 2014.
2. Мельников В. П. Информационная безопасность и защита информации. - М.: Академия, 2008.
3. Алферов А.П., Зубов А.Ю. и др. Основы криптографии: Учеб. пособие, 2-е изд., испр. и доп. М.: Гелиос АРВ, 2002.- 480 с.: ил.

6.3 Периодические издания

1. Вестник Омского университета [Текст]: ежекварт. науч. журнал/ Мин-во образ. и науки РФ, Омский гос. ун-т. – Омск, 2013-2016
2. Известия ВУЗ. Физика [Текст]: ежемес. науч. журнал/ Мин-во образ. и науки РФ, Томский гос. ун-т. - Томск: Сиб. физико-технич. ин-т, 2012-2018
3. Известия ТулГУ. Естественные науки [Текст]: ежемес. науч. журнал/ Мин-во образ. и науки РФ, Тульский гос. ун-т. - Тула, 2008-2015

7 Перечень ресурсов информационно-телекоммуникационной сети "Интернет" (далее - сеть "Интернет"), необходимых для освоения дисциплины (модуля)

1. Institute of Electrical and Electronics Engineers [Electronic resource]. — Mode of access: <http://www.ieee.org>, free.
2. Национальная ассоциация управления проектами «Совнет» [Электронный ресурс]. — Режим доступа: <http://www.sovnet.ru>, свободный.
3. Project Management Resource Center [Electronic resource]. — Mode of access: <http://www.allpm.com>, free.

4. Project Management Forum [Electronic resource]. — Mode of access: <http://www.pmforum.org>, free.
5. International Project Management Association [Electronic resource]. — Mode of access: <http://www.ipma.ch>, free.
2. Project Management Institute [Electronic resource]. — Mode of access: <http://www.pmi.org>, free.
3. Institute of Advanced Projects and Contracts Management [Electronic resource]. — Mode of access: <http://www.epci.no>, free.
4. Project Management com [Electronic resource]. — Mode of access: <http://www.projectmanagement.com>, free.
5. Project Management Center [Electronic resource]. — Mode of access: <http://www.infogoal.com>, free.
6. Center for International Projects and Project Management [Electronic resource]. — Mode of access: <http://www.iol.ie/~mattewar/CIPPM>, free.
7. Project Connections Newsletter [Electronic resource]. — Mode of access: <http://projectconnections.com/newsletter>, free.
8. The NASA Academy of program/project and engineering leadership [Electronic resource]. — Mode of access: <http://www.nasa.gov/offices/ocp/appel/home/index.html>, free.

8 Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине (модулю), включая перечень программного обеспечения и информационных справочных систем (при необходимости)

1. Пакет программного обеспечения «MS Office».
2. Пакет программного обеспечения «Mathcad».

9 Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине (модулю)

№ п/п	Наименование вида образования, уровня образования, профессии, специальности, направления подготовки (для профессионального образования), подвида дополнительного образования	Наименование оборудованных учебных кабинетов, объектов для проведения практических занятий, объектов физической культуры и спорта с перечнем основного оборудования	Адрес (местоположение) учебных кабинетов, объектов для проведения практических занятий, объектов физической культуры и спорта (с указанием номера помещения в соответствии с документами бюро технической инвентаризации)
15.14	Физика	Учебная аудитория для проведения занятий лекционного типа: стол преподавательский – не менее 1 шт., доска учебная – не менее 1 шт., экран проекционный – не менее 1 шт., мультимедиа проектор не менее 1 шт., учебные парты - не менее 14 шт., лабораторные столы - не менее 8 шт., стул - не менее 38 шт., плакат - не менее 10 шт., стенд – не менее 1 шт., шкаф – не менее 1 шт., стеллаж – не менее 1 шт., учебное оборудование: МУК М1 - не менее 2 шт., МУК М2 - не менее 2 шт., МУК ОВ - не менее 1 шт., МУК О - не менее 1 шт., МУК ЭМ - не менее 1 шт.	644099, г.Омск, ул. Ивана Алексеева, д. 2 (№№ 52, 53, 54, 55, 56 на поэтажном плане (1П), 4 этаж)
		Учебная аудитория для проведения занятий семинарского типа: стол преподавательский – не менее 1 шт., доска учебная – не менее 1 шт., экран проекционный – не менее 1 шт., мультимедиа проектор не менее 1 шт., учебные парты - не менее 14 шт., лабораторные столы - не менее 8 шт., стул - не менее 38 шт., плакат - не менее 10 шт., стенд – не менее 1 шт., шкаф – не менее 1 шт., стеллаж – не менее 1 шт., учебное оборудование: МУК М1 - не менее 2 шт., МУК М2 - не менее 2 шт., МУК ОВ - не менее 1 шт., МУК О - не менее 1 шт., МУК ЭМ - не менее 1 шт.	
		Лаборатория физики: стол преподавательский – не менее 1 шт., доска учебная – не менее 1 шт., экран проекционный – не менее 1 шт., мультимедиа проектор не менее 1 шт., учебные парты - не менее 14 шт., лабораторные столы - не менее 8 шт., стул - не менее 38 шт., плакат - не менее 10 шт., стенд – не менее 1 шт., шкаф – не менее 1 шт., стеллаж – не менее 1 шт., учебное оборудование: МУК М1 - не менее 2 шт., МУК М2 - не менее 2 шт., МУК ОВ - не менее 1 шт., МУК О - не менее 1 шт., МУК ЭМ - не менее 1 шт.	
		Учебная аудитория для проведения текущего контроля и промежуточной аттестации: стол преподавательский – не менее 1 шт., доска учебная – не менее 1 шт., экран проекционный – не менее 1 шт., мультимедиа проектор не менее 1 шт., учебные парты - не менее 14 шт., лабораторные столы - не менее 8 шт., стул - не менее 38 шт., плакат - не менее 10 шт., стенд – не менее 1 шт., шкаф – не менее 1 шт., стеллаж – не менее 1 шт., учебное оборудование: МУК М1 - не менее 2 шт., МУК М2 - не менее 2 шт., МУК ОВ - не менее 1 шт., МУК О - не менее 1 шт., МУК ЭМ - не менее 1 шт.	

		Учебная аудитория для проведения групповых и индивидуальных консультаций: ученическая парта - не менее 21 шт., стол преподавательский - не менее 1 шт., доска учебная - не менее 1 шт., экран проекционный - не менее 1 шт., стул - не менее 43 шт., рамки портретные - не менее 6 шт., плакаты - не менее 5 шт.	644099, г.Омск, ул. Ивана Алексеева, д. 2 (№№ 31,32 на поэтажном плане (1П), 4 этаж)
		Помещение для самостоятельной работы: операционная система Windows, пакет программ Microsoft Office, СПС Консультант ПЛЮС, ГАРАНТ, доска - не менее 2 шт., экран - не менее 2 шт., шкаф - не менее 2 шт, стенды - не менее 10 шт., стол - не менее 43 шт., стул - не менее 48 шт.	644099, г. Омск, ул. Ивана Алексеева, д. 2 (№№ 52, 53,54,55 на поэтажном плане (1П), 3 этаж)